

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-260522

(43)Date of publication of application : 16.09.2004

(51)Int.Cl.

H04N 5/92  
G09C 1/00  
H04N 7/08  
H04N 7/081  
H04N 7/167

(21)Application number : 2003-048643

(71)Applicant : NIPPON HOSO KYOKAI <NHK>

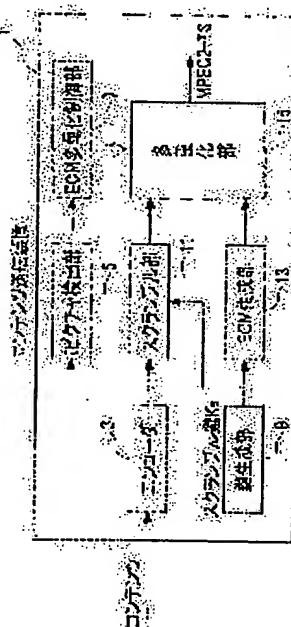
(22)Date of filing : 26.02.2003

(72)Inventor : NISHIMOTO TOMONARI  
KURIOKA TATSUYA  
BABA AKITSUGU  
FUJII ARISA

(54) CONTENT TRANSMITTER, CONTENT TRANSMISSION METHOD, CONTENT TRANSMISSION PROGRAM, CONTENT REPRODUCING DEVICE, CONTENT REPRODUCING METHOD AND CONTENT REPRODUCING PROGRAM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a content transmitter, transmission method, transmission program, and a content reproducing device, method and program that can maintain the high performance of the fast forward reproduction and fast rewinding reproduction (special reproduction) of ciphered contents without the risk of being a scramble key Ks (cipher key) illicitly acquired and which stabilize an operation.  
SOLUTION: A content transmitter 1 for transmitting ciphered contents so that the ciphered contents can be reproduced on a reception side is provided with an encoder 3, an I picture detection part 5, an ECM multiplex control part 7, a key generation part 9, a descramble part 11, an ECM generation part 13 and a multiplex part 15.



(19) 日本国特許庁 (JP)

## (12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-260522

(P2004-260522A)

(43) 公開日 平成16年9月16日 (2004. 9. 16)

(51) Int. Cl. <sup>7</sup>	F I	テーマコード (参考)
H04N 5/92	H04N 5/92 H	5C053
G09C 1/00	G09C 1/00 660D	5C063
H04N 7/08	H04N 7/167 Z	5C064
H04N 7/081	H04N 7/08 Z	5J104
H04N 7/167		

審査請求 未請求 請求項の数 6 O L (全 19 頁)

(21) 出願番号 特願2003-48643 (P2003-48643)  
 (22) 出願日 平成15年2月26日 (2003. 2. 26)

(71) 出願人 000004352  
 日本放送協会  
 東京都渋谷区神南2丁目2番1号  
 (74) 代理人 100064414  
 弁理士 磯野 道造  
 (72) 発明者 西本 友成  
 東京都世田谷区砦一丁目10番11号  
 日本放送協会 放送技術研究  
 所内  
 (72) 発明者 栗岡 辰弥  
 東京都世田谷区砦一丁目10番11号  
 日本放送協会 放送技術研究  
 所内

最終頁に続く

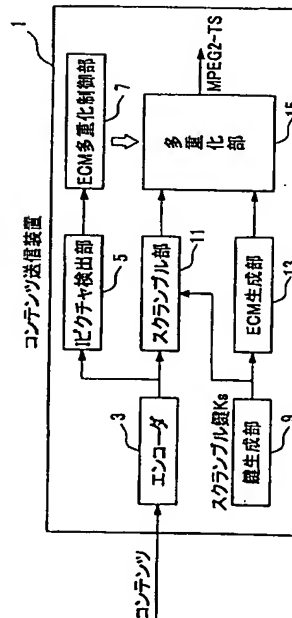
(54) 【発明の名称】 コンテンツ送信装置、コンテンツ送信方法、コンテンツ送信プログラムおよびコンテンツ再生装置、コンテンツ再生方法、コンテンツ再生プログラム

## (57) 【要約】

【課題】 スクランブル鍵K<sub>s</sub> (暗号鍵) を不正に取得される恐れがなく、暗号化コンテンツの早送り再生や早巻き戻し再生 (特殊再生) の性能を高性能に維持し、動作を安定させることができるコンテンツ送信装置、方法、プログラムおよびコンテンツ再生装置、方法、プログラムを提供する。

【解決手段】 コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信装置1であって、エンコーダ3と、Iピクチャ検出部5と、ECM多重化制御部7と、鍵生成部9と、デスクランブル部11と、ECM生成部13と、多重化部15と、を備えた。

【選択図】 図1



## 【特許請求の範囲】

## 【請求項 1】

コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信装置であって、

前記コンテンツを符号化して符号化コンテンツとするコンテンツ符号化手段と、

このコンテンツ符号化手段で前記コンテンツを符号化する際の基準となる基準コンテンツを前記符号化コンテンツから検出する基準コンテンツ検出手段と、

前記符号化コンテンツを暗号鍵で暗号化して暗号化コンテンツとする符号化コンテンツ暗号化手段と、

前記暗号鍵を含む暗号鍵関連情報を暗号化して、前記暗号化コンテンツを受信側でリアルタイム再生するための受信用 ECM と、前記暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用 ECM とを生成する ECM 生成手段と、

前記基準コンテンツに基づいて、前記蓄積再生用 ECM を前記暗号化コンテンツに多重化する際の多重化制御信号を生成する多重化制御信号生成手段と、

前記多重化制御信号に基づいて、前記暗号化コンテンツと、前記受信用 ECM と、前記蓄積再生用 ECM とを多重化して多重化コンテンツとする暗号化コンテンツ多重化手段と、を備えることを特徴とするコンテンツ送信装置。

## 【請求項 2】

コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信方法であって、

前記コンテンツを符号化して符号化コンテンツとするコンテンツ符号化ステップと、

このコンテンツ符号化ステップにおいて前記コンテンツを符号化する際の基準となる基準コンテンツを前記符号化コンテンツから検出する基準コンテンツ検出ステップと、

前記符号化コンテンツを暗号鍵で暗号化して暗号化コンテンツとする符号化コンテンツ暗号化ステップと、

前記暗号鍵を含む暗号鍵関連情報を暗号化して、前記暗号化コンテンツを受信側でリアルタイム再生するための受信用 ECM と、前記暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用 ECM とを生成する ECM 生成ステップと、

前記基準コンテンツに基づいて、前記蓄積再生用 ECM を前記暗号化コンテンツに多重化する際の多重化制御信号を生成する多重化制御信号生成ステップと、

前記多重化制御信号に基づいて、前記暗号化コンテンツと、前記受信用 ECM と、前記蓄積再生用 ECM とを多重化して多重化コンテンツとする暗号化コンテンツ多重化ステップと、

を含むことを特徴とするコンテンツ送信方法。

## 【請求項 3】

コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信する装置を、

前記コンテンツを符号化して符号化コンテンツとするコンテンツ符号化手段、

このコンテンツ符号化手段で前記コンテンツを符号化する際の基準となる基準コンテンツを前記符号化コンテンツから検出する基準コンテンツ検出手段、

前記符号化コンテンツを暗号鍵で暗号化して暗号化コンテンツとする符号化コンテンツ暗号化手段、

前記暗号鍵を含む暗号鍵関連情報を暗号化して、前記暗号化コンテンツを受信側でリアルタイム再生するための受信用 ECM と、前記暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用 ECM とを生成する ECM 生成手段、

前記基準コンテンツに基づいて、前記蓄積再生用 ECM を前記暗号化コンテンツに多重化する際の多重化制御信号を生成する多重化制御信号生成手段、

前記多重化制御信号に基づいて、前記暗号化コンテンツと、前記受信用 ECM と、前記蓄積再生用 ECM とを多重化して多重化コンテンツとする暗号化コンテンツ多重化手段、として機能させることを特徴とするコンテンツ送信プログラム。

## 【請求項 4】

請求項 1 に記載のコンテンツ送信装置から送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生装置であって、  
前記多重化コンテンツを受信して、前記受信用 E C M と、前記蓄積再生用 E C M および前記暗号化コンテンツとに分離する多重化コンテンツ受信分離手段と、  
前記受信用 E C M および前記蓄積再生用 E C M を復号して前記暗号鍵を取得する E C M 復号手段と、  
前記蓄積再生用 E C M および前記暗号化コンテンツを蓄積する蓄積手段と、  
この蓄積手段に蓄積されている前記蓄積再生用 E C M および前記暗号化コンテンツを分離する分離手段と、  
前記暗号化コンテンツを前記 E C M 復号手段にて取得された暗号鍵で復号し、前記符号化コンテンツとする暗号化コンテンツ復号手段と、  
この暗号化コンテンツ復号手段で復号された符号化コンテンツを前記コンテンツに復元するコンテンツ復元手段と、  
を備えることを特徴とするコンテンツ特殊再生装置。

【請求項 5】

請求項 2 に記載のコンテンツ送信方法によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生方法であって、  
前記多重化コンテンツを受信して、前記受信用 E C M と、前記蓄積再生用 E C M および前記暗号化コンテンツとに分離する多重化コンテンツ受信分離ステップと、  
前記受信用 E C M および前記蓄積再生用 E C M を復号して前記暗号鍵を取得する E C M 復号ステップと、  
前記蓄積再生用 E C M および前記暗号化コンテンツを蓄積装置に蓄積させるための蓄積ステップと、  
前記蓄積装置に蓄積されている前記蓄積再生用 E C M および前記暗号化コンテンツを分離する分離ステップと、  
前記暗号化コンテンツを前記 E C M 復号ステップにて取得された暗号鍵で復号し、前記符号化コンテンツとする暗号化コンテンツ復号ステップと、  
この暗号化コンテンツ復号ステップにて復号された符号化コンテンツを前記コンテンツに復元するコンテンツ復元ステップと、  
を含むことを特徴とするコンテンツ特殊再生方法。

【請求項 6】

請求項 3 に記載のコンテンツ送信プログラムが機能する装置によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生する装置を、  
前記多重化コンテンツを受信して、前記受信用 E C M と、前記蓄積再生用 E C M および前記暗号化コンテンツとに分離する多重化コンテンツ受信分離手段、  
前記受信用 E C M および前記蓄積再生用 E C M を復号して前記暗号鍵を取得する E C M 復号手段、  
前記蓄積再生用 E C M および前記暗号化コンテンツを蓄積装置に蓄積させるための蓄積手段、  
前記蓄積装置に蓄積されている前記蓄積再生用 E C M および前記暗号化コンテンツを分離する分離手段、  
前記暗号化コンテンツを前記 E C M 復号手段で取得された暗号鍵で復号し、前記符号化コンテンツとする暗号化コンテンツ復号手段、  
この暗号化コンテンツ復号手段で復号された符号化コンテンツを前記コンテンツに復元するコンテンツ復元手段、  
として機能させることを特徴とするコンテンツ特殊再生プログラム。

【発明の詳細な説明】

## 【 0 0 0 1 】

## 【 発明の属する技術分野 】

本発明は、コンテンツを暗号化した暗号化コンテンツを送信するコンテンツ送信装置、コンテンツ送信方法、コンテンツ送信プログラムおよび暗号化コンテンツを受信して再生するコンテンツ再生装置、コンテンツ再生方法、コンテンツ再生プログラムに関する。

## 【 0 0 0 2 】

## 【 従来技術 】

一般に、現行のデジタル放送では、秒単位（数秒程度）の時間で変更される暗号鍵（スクランブル鍵  $K_s$ ）を用いて、デジタルコンテンツを暗号化（スクランブル）し暗号化コンテンツとして放送している。このスクランブル鍵  $K_s$  も暗号化され、ECM（Entitlement Element Control Message；共通情報）として、暗号化コンテンツに一定間隔で多重化されている。このECMが暗号化コンテンツに一定間隔で多重化される多重間隔は、図9に示したように、例えば、100ms程度の間隔（図9中、ECM1同士の間隔）である（非特許文献1を参照）。この多重間隔は、デジタル放送の放送帯域を有効に利用するためには、できる限り長い方が良いが、チャンネル選局時の応答速度を考慮すると短い方が良くするために、長すぎず短すぎず適当な間隔に設定されたものである。

## 【 0 0 0 3 】

そして、秒単位の時間で変更されるスクランブル鍵  $K_s$  で暗号化された暗号化コンテンツは、受信側のデジタル受信機で受信された時に、暗号が解除、すなわち復号されてデジタルコンテンツとされ、当該デジタル受信機に備えられるローカルな暗号鍵が用いられて、復号されたデジタルコンテンツが再暗号化されて、デジタル受信機に内蔵されている記録装置か外部の蓄積装置に蓄積される（以下、デジタル受信機に内蔵されている記録装置を、デジタル受信機と、外部の蓄積装置を、蓄積装置と略称することにする）。

## 【 0 0 0 4 】

しかし、デジタル受信機や蓄積装置は、暗号化コンテンツを復号したり、一旦復号されたデジタルコンテンツを再暗号化して蓄積したりしているので、不正利用を行う目的で改造された（製造された）デジタル受信機（不正デジタル受信機）では、デジタルコンテンツが不正に利用されるおそれ（デジタルコンテンツ不正利用）が生じる。このデジタルコンテンツ不正利用を防止するために、デジタル受信機で受信時に復号せずに、暗号化コンテンツのまま蓄積する様々な方法が提案されている。

## 【 0 0 0 5 】

ところで、デジタル受信機で受信時に復号せずに、暗号化コンテンツのまま蓄積した場合、当該デジタル受信機や蓄積装置には、蓄積された暗号化コンテンツの通常再生だけではなく、早送り再生や早巻き戻し再生等の特殊再生を可能にする必要がある（特許文献1参照）。

## 【 0 0 0 6 】

例えば、MPEG2-TS形式（トランスポートストリーム）のデジタルコンテンツを暗号化した暗号化コンテンツを早送り再生や早巻き戻し再生する場合には、スクランブル鍵  $K_s$  が含まれている共通情報であるECMを検索し、この検索したECMをICカード等によって構成されるセキュリティモジュール内で復号し、この復号して得られたスクランブル鍵  $K_s$  を用いて、暗号化コンテンツを復号しながら、Iピクチャ、Pピクチャ、Bピクチャのうち、Iピクチャを検索して、このIピクチャのみを順次再生することで実現している。

## 【 0 0 0 7 】

ここで、暗号化されていないデジタルコンテンツ（MPEG2-TS形式）の早送り再生、早巻き戻し再生について述べておくと、Iピクチャ、Pピクチャ、Bピクチャのうち、Iピクチャのみを順次再生するか、Iピクチャを数枚スキップしながら順次再生して、早送り再生、早巻き戻し再生を実現する。また、デジタル受信機で一旦蓄積し、デジタル受信機または蓄積装置にて、ローカルな暗号鍵で暗号化された再暗号化コンテンツを早送り再生や、早巻き戻し再生する場合には、ローカルな暗号鍵を取得して、おおよそのIピク

チャの位置までスキップして、取得したローカルな暗号鍵で復号しながら、Iピクチャを検索し、この検索したIピクチャのみを順次再生することで実現する。

【0008】

【非特許文献1】

「デジタル放送における限定受信方式」 標準規格 ARIB STD-B25 p 7, p 17 ~ p 19

【特許文献1】

特開2002-247547号公報（段落71～77、第21図）

【0009】

【発明が解決しようとする課題】

しかしながら、従来の方式では、MPEG2のVideoストリームとは非同期にECMが暗号化コンテンツに多重化されており、当該暗号化コンテンツの早送り再生や早巻き戻し再生を実行した場合、ECMとIピクチャの間隔が変動しているため、スクランブル鍵Ksを用いて暗号化コンテンツを復号しながらIピクチャを検索すると、この検索するための処理時間が変動することになり、暗号化コンテンツの早送り再生や早巻き戻し再生の動作が不安定になるという問題がある。

【0010】

また、ECMとIピクチャの間隔は、ECMの送出間隔に依存し、ECMの送出間隔が長くなるほど、Iピクチャを検索するための処理時間が増大するので、暗号化コンテンツの早送り再生や早巻き戻し再生の性能は、ECMの送出間隔に多大な影響を受けることになるという問題がある。

【0011】

さらに、スクランブルされたVideoストリームをデスクランブルせずに、Iピクチャを検索するために、VideoストリームのTSパケットのヘッダ等の非暗号化部に、当該TSパケットがIピクチャであることを示す情報を入れ込む技術がある。この技術によって、Iピクチャの検索時間を短くすることが可能であるが、スクランブルされたVideoストリームにおいて、デジタルコンテンツ不正利用を実行する不正行為者に、少なくともIピクチャであることを知らしめてしまうことになり、当該不正行為者にスクランブル鍵Ksが不正に取得される恐れがあるという問題がある。

【0012】

さらにまた、特許文献1に記載されている方式では、複数のスクランブル鍵Ksをまとめて、スクランブル鍵KsリストとしてECMに挿入することにより、スクランブル鍵Ksを検索するまでの処理時間を短縮し、早送り再生や早巻き戻し再生の性能を向上させるものであるが、スクランブル鍵Ksリストの送出間隔を短くすると、放送帯域を不効率に使用することになり、長くすると、暗号化コンテンツの途中のみを記録した場合に暗号化コンテンツが再生できなくなってしまうという問題がある。

【0013】

そこで、本発明の目的は、前記した従来の技術が有する課題を解消し、スクランブル鍵Ks（暗号鍵）を不正に取得される恐れがなく、暗号化コンテンツの早送り再生や早巻き戻し再生（特殊再生）の性能を高性能に維持し、動作を安定させることができるコンテンツ送信装置、コンテンツ送信方法、コンテンツ送信プログラムおよびコンテンツ再生装置、コンテンツ再生方法、コンテンツ再生プログラムを提供することにある。

【0014】

【課題を解決するための手段】

本発明は、前記した目的を達成するため、以下に示す構成とした。

請求項1記載のコンテンツ送信装置は、コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信装置であって、コンテンツ符号化手段と、基準コンテンツ検出手段と、符号化コンテンツ暗号化手段と、ECM生成手段と、多重化制御信号生成手段と、暗号化コンテンツ多重化手段と、を備える構成とした。

【0015】

かかる構成によれば、コンテンツ送信装置は、まず、コンテンツ符号化手段によって、コンテンツを符号化して、符号化コンテンツとする。この符号化コンテンツは、例えば、MPEG等によって圧縮符号化されたものである。続いて、コンテンツ送信装置は、コンテンツ符号化手段によってコンテンツを符号化する際の基準となる基準コンテンツを、基準コンテンツ検出手段によって、符号化コンテンツから検出する。基準コンテンツは、例えば、MPEGにおけるIピクチャ（フレーム内符号化画像）である。

【0016】

そして、コンテンツ送信装置は、符号化コンテンツ暗号化手段によって、符号化コンテンツを暗号鍵で暗号化して、暗号化コンテンツとし、ECM生成手段によって、暗号鍵を含む暗号鍵関連情報を暗号化して、暗号化コンテンツを受信側でリアルタイム再生するための受信用ECMと、暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ECMとを生成する。

【0017】

また、コンテンツ送信装置は、基準コンテンツに基づいて、蓄積再生用ECMを暗号化コンテンツに多重する際の多重化制御信号を多重化制御信号生成手段によって生成し、暗号化コンテンツ多重化手段によって、多重化制御信号に基づいて、暗号化コンテンツと、受信用ECMと、蓄積再生用ECMとを多重化して、多重化コンテンツとする。

【0018】

なお、受信用ECMと蓄積再生用ECMとは、実質的に同じものであってもいいが、蓄積再生用ECMは、多重化制御信号に基づいて、暗号化コンテンツ多重化手段で多重化される際の多重化位置が、受信用ECMの多重化位置とは異なるように制御されるものである。

【0019】

請求項2記載のコンテンツ送信方法は、コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信するコンテンツ送信方法であって、コンテンツ符号化ステップと、基準コンテンツ検出ステップと、符号化コンテンツ暗号化ステップと、ECM生成ステップと、多重化制御信号生成ステップと、暗号化コンテンツ多重化ステップと、を含むものとした。

【0020】

この方法によれば、コンテンツ送信方法は、まず、コンテンツ符号化ステップにおいて、コンテンツを符号化して、符号化コンテンツとし、コンテンツ符号化ステップにてコンテンツを符号化する際の基準となる基準コンテンツを、基準コンテンツ検出ステップにおいて符号化コンテンツから検出する。続いて、コンテンツ送信方法は、符号化コンテンツ暗号化ステップにおいて、符号化コンテンツを暗号鍵で暗号化し、暗号化コンテンツとし、ECM生成ステップにおいて、暗号鍵を含む暗号鍵関連情報を暗号化することによって、暗号化コンテンツを受信側でリアルタイム再生するための受信用ECMと、暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ECMとを生成する。

【0021】

また、コンテンツ送信方法は、多重化制御信号生成ステップにおいて、基準コンテンツに基づいて、蓄積再生用ECMを暗号化コンテンツに多重する際の多重化制御信号を生成し、暗号化コンテンツ多重化ステップにおいて、多重化制御信号に基づいて、暗号化コンテンツと、受信用ECMと、蓄積再生用ECMとを多重化して、多重化コンテンツとする。

【0022】

請求項3記載のコンテンツ送信プログラムは、コンテンツを暗号化した暗号化コンテンツを受信側で再生可能に送信する装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、コンテンツ符号化手段、基準コンテンツ検出手段、符号化コンテンツ暗号化手段、ECM生成手段、多重化制御信号生成手段、暗号化コンテンツ多重化手段、である。

【0023】

かかる構成によれば、コンテンツ送信プログラムは、コンテンツ符号化手段によって、コ

10

20

30

40

50

ンテンツを符号化して、符号化コンテンツとし、コンテンツ符号化手段によってコンテンツを符号化する際の基準となる基準コンテンツを、基準コンテンツ検出手段によって、符号化コンテンツから検出する。続いて、コンテンツ送信プログラムは、符号化コンテンツ暗号化手段によって、符号化コンテンツを暗号鍵で暗号化して、暗号化コンテンツとし、ECM生成手段によって、暗号鍵を含む暗号鍵関連情報を暗号化することにより、暗号化コンテンツを受信側でリアルタイム再生するための受信用ECMと、暗号化コンテンツを受信側で蓄積後に再生するための蓄積再生用ECMとを生成する。

#### 【0024】

そして、コンテンツ送信プログラムは、多重化制御信号生成手段によって、基準コンテンツに基づいて、蓄積再生用ECMを暗号化コンテンツに多重する際の多重化制御信号を生成し、暗号化コンテンツ多重化手段によって、多重化制御信号に基づいて、暗号化コンテンツと、受信用ECMと、蓄積再生用ECMとを多重化して、多重化コンテンツとする。

#### 【0025】

請求項4記載のコンテンツ再生装置は、請求項1に記載のコンテンツ送信装置から送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生装置であって、多重化コンテンツ受信分離手段と、ECM復号手段と、蓄積手段と、分離手段と、暗号化コンテンツ復号手段と、コンテンツ復元手段と、を備える構成とした。

#### 【0026】

かかる構成によれば、コンテンツ再生装置は、多重化コンテンツ受信分離手段によって、多重化コンテンツを受信し、受信用ECMと、蓄積再生用ECMおよび暗号化コンテンツとに分離し、ECM復号手段によって、受信用ECMおよび蓄積再生用ECMを復号して、暗号鍵を取得する。続いて、コンテンツ再生装置は、蓄積手段によって、蓄積再生用ECMおよび暗号化コンテンツを蓄積し、分離手段によって、この蓄積手段に蓄積されている蓄積再生用ECMおよび暗号化コンテンツを分離する。

#### 【0027】

そして、コンテンツ再生装置は、暗号化コンテンツ復号手段によって、暗号化コンテンツをECM復号手段にて取得された暗号鍵で復号し、符号化コンテンツとし、コンテンツ復元手段によって、この暗号化コンテンツ復号手段にて復号された符号化コンテンツをコンテンツに復元する。なお、多重化コンテンツを受信した後、すぐに再生する場合は、受信用ECMのみ復号し、暗号鍵を取得して、暗号化コンテンツを暗号化コンテンツ復号手段によって復号し、コンテンツ復元手段によって復元する。

#### 【0028】

請求項5記載のコンテンツ再生方法は、請求項2に記載のコンテンツ送信方法によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生するコンテンツ再生方法であって、多重化コンテンツ受信分離ステップと、ECM復号ステップと、蓄積ステップと、分離ステップと、暗号化コンテンツ復号ステップと、コンテンツ復元ステップと、を含むものとした。

#### 【0029】

この方法によれば、コンテンツ再生方法は、多重化コンテンツ受信分離ステップにおいて、多重化コンテンツを受信して、受信用ECMと、蓄積再生用ECMおよび暗号化コンテンツとに分離し、ECM復号ステップにおいて、受信用ECMおよび蓄積再生用ECMを復号して暗号鍵を取得する。続いて、コンテンツ再生方法は、蓄積ステップにおいて、蓄積再生用ECMおよび暗号化コンテンツを蓄積装置に蓄積し、分離ステップにおいて、蓄積装置に蓄積されている蓄積再生用ECMおよび暗号化コンテンツを分離する。

#### 【0030】

そして、コンテンツ再生方法は、暗号化コンテンツ復号ステップにおいて、暗号化コンテンツをECM復号ステップにて取得された暗号鍵で復号し、符号化コンテンツとし、コン

10

20

30

40

50



テンツ復元ステップにおいて、暗号化コンテンツ復号ステップにて復号した符号化コンテンツをコンテンツに復元する。

【0031】

請求項6記載のコンテンツ再生プログラムは、請求項3に記載のコンテンツ送信プログラムが機能する装置によって送信された多重化コンテンツを受信して、当該多重化コンテンツに含まれている暗号化コンテンツを符号化コンテンツに復号し、当該符号化コンテンツを復元したコンテンツを再生する装置を、以下に示す手段として機能させることを特徴とする。当該装置を機能させる手段は、多重化コンテンツ受信分離手段、ECM復号手段、蓄積手段、分離手段、暗号化コンテンツ復号手段、コンテンツ復元手段、である。

【0032】

かかる構成によれば、コンテンツ再生プログラムは、多重化コンテンツ受信分離手段によって、多重化コンテンツを受信し、受信用ECMと、蓄積再生用ECMおよび暗号化コンテンツとに分離し、ECM復号手段によって、受信用ECMおよび蓄積再生用ECMを復号して、暗号鍵を取得する。続いて、コンテンツ再生プログラムは、蓄積手段によって、蓄積再生用ECMおよび暗号化コンテンツを蓄積装置に蓄積し、分離手段によって、この蓄積装置に蓄積している蓄積再生用ECMおよび暗号化コンテンツを分離する。

【0033】

そして、コンテンツ再生プログラムは、暗号化コンテンツ復号手段によって、暗号化コンテンツをECM復号手段にて取得した暗号鍵で復号し、符号化コンテンツとする。コンテンツ復元手段によって、この暗号化コンテンツ復号手段にて復号した符号化コンテンツをコンテンツに復元する。

【0034】

【発明の実施の形態】

以下、本発明の一実施の形態について、図面を参照して詳細に説明する。

(コンテンツ送信装置の構成)

図1にコンテンツ送信装置のブロック図を示す。この図1に示すように、コンテンツ送信装置1は、エンコーダ3と、Iピクチャ検出部5と、ECM多重化制御部7と、鍵生成部9と、スクランブル部11と、ECM生成部13と、多重化部15とを備えている。

【0035】

このコンテンツ送信装置1は、映像音声等のコンテンツを暗号化し、この暗号化した暗号化コンテンツの任意の場所を、受信側で、不連続に再生できるように（特殊再生可能に）して、送信するものである。

【0036】

エンコーダ3は、入力された映像音声等のコンテンツ（以下、映像音声コンテンツという）をエンコードする（符号化する）ものである。このエンコーダ3のエンコード（符号化）によって、映像音声コンテンツは、MPEG2形式の映像音声コンテンツストリーム（TS）とされる。なお、エンコードとは、映像音声信号（映像音声コンテンツ）からデジタル符号を生成することであり、エンコードの目的は、アナログ信号をデジタル信号に変換することや、デジタル信号の冗長度を減らすことで、元の信号を圧縮して伝送または蓄積されるデータ量を減少させることである。このエンコーダ3が特許請求の範囲に記載したコンテンツ符号化手段に相当するものであり、MPEG2形式の映像音声コンテンツストリーム（TS）が符号化コンテンツに相当するものである。

【0037】

また、MPEG2形式の映像音声コンテンツストリームは、Iピクチャ、Pピクチャ、Bピクチャの3種類のピクチャに分けることができ、Iピクチャがエンコードする前のコンテンツの一画像（そのまま（当初）の画像）であり、符号化する際の基準となるものである。このIピクチャが特許請求の範囲に記載した基準コンテンツに相当するものである。

【0038】

また、このMPEG2形式の映像音声コンテンツストリームは、厳密に言うと映像信号がMPEG2 Video、音声信号がMPEG2 Audio AACと呼ばれる符号化

10

20

30

40

50

方式で圧縮されたものであり、ES (Elementary Stream)、PES (Packetized Elementary Stream) に変換されているものである。字幕や文字スーパーの情報はPES形式に、その他のデータはセクション (Section) と呼ばれる形式に変換されている。これらPES形式およびセクション形式の信号は、セクション形式のPSI (Program Specific Information、番組特定情報) およびSI (Service Information、番組配列情報) のチャンネル・番組情報と共にまとめられている。

#### 【0039】

そして、このPSIに含まれている情報には、PAT (Program Association Table) と、PMT (Program Map Table) とが含まれている (なお、PSIに含まれている別の情報であるNIT (Network Information Table)、CAT (Conditional Access Table) については説明を省略) 10

#### 【0040】

PATはTS内に含まれている全PMTのPID (Packet Identifier、パケット識別) を示すものであり、PMTは、1個の編成チャンネルを構成するコンポーネント (映像、音声、データ等) のPID、つまり、stream\_type等を示すものである。

#### 【0041】

Iピクチャ検出部5は、エンコーダ3でエンコードされた映像音声コンテンツであるMP 20  
EG2形式の映像音声コンテンツストリーム (TSパケット) から、Iピクチャの先頭パケットを含んでいるTSパケットを検出するものである。つまり、このIピクチャ検出部5では、Iピクチャの先頭パケットを含んでいるTSパケットを検出することで、MPEG2形式の映像音声コンテンツストリーム (TSパケット) に含まれている各Iピクチャの正確な位置を取得するものである。このIピクチャ検出部5が特許請求の範囲に記載した基準コンテンツ検出手段に相当するものである。

#### 【0042】

ECM多重化制御部7は、Iピクチャ検出部5で検出されたIピクチャに同期させて、E 30  
CM生成部13で生成された受信用ECM、蓄積再生用ECMを多重化部15で多重化する際の多重化タイミングを制御する多重化制御信号を生成し、当該多重化部15に出力して、多重化部15を制御するものである。なお、このECM多重化制御部7が特許請求の範囲に記載した多重化制御信号生成手段に相当するものである。

#### 【0043】

鍵生成部9は、映像音声コンテンツを暗号化するための秘密鍵であるスクランブル鍵Ksを生成するものである。このスクランブル鍵Ksは、数秒単位 (通常1秒) で更新されるものであり、この鍵生成部9では、この更新時刻に合わせて、スクランブル鍵Ksが生成される。

#### 【0044】

スクランブル部11は、エンコーダ3でエンコードされた映像音声コンテンツストリーム (TS) をスクランブル鍵Ksでスクランブルして、暗号化コンテンツを生成するもので 40  
ある。なお、このスクランブル部11が特許請求の範囲に記載した符号化コンテンツ暗号化手段に相当するものであり、スクランブル鍵Ksが暗号鍵に相当するものである。

#### 【0045】

ECM生成部13は、送信側と受信側との間で予め共通に保持している秘密鍵 (例えば、ワーク鍵Kw、マスタ鍵Km等) によって、スクランブル鍵Ksを含む暗号鍵関連情報を暗号化し、ECM (ECM; Entitlement Control Message : 共通情報、受信用ECMおよび蓄積再生用ECM) を生成するものである。このECM 50  
生成部13でECM (受信用ECMおよび蓄積再生用ECM) を生成する際に、「table\_id\_extension」を「0x0000」とする受信用ECMと、「table\_id\_extension」を「0x0001」とする蓄積再生用ECMとが生成

され、多重化部 15 に出力される。

【0046】

受信用 ECM は、受信側で暗号化コンテンツを受信しながら、当該暗号化コンテンツを復号する際（リアルタイム再生するため）に使用するものであり、蓄積再生用 ECM は、受信側で一旦暗号化コンテンツを受信して蓄積した後、当該暗号化コンテンツを復号する際に使用するものである。

【0047】

また、スクランブル鍵  $K_s$  を含む暗号鍵関連情報とは、スクランブル鍵  $K_s$  と、映像音声コンテンツを提供した事業者 ID、つまり放送局、コンテンツ制作会社等の識別情報とを含む情報のことである。なお、この ECM 生成部 13 が特許請求の範囲に記載した ECM 生成手段に相当するものである。

【0048】

多重化部 15 は、スクランブル部 11 で暗号化された暗号化コンテンツと、ECM 生成部 13 で生成された受信用 ECM および蓄積再生用 ECM とを、ECM 多重化制御部 7 で生成された多重化制御信号に基づいて多重化し、多重化コンテンツ（MPEG2-TS）として出力するものである。なお、この多重化部 15 が特許請求の範囲の請求項に記載した暗号化コンテンツ多重化手段に相当するものである。

【0049】

また、この多重化部 15 で蓄積再生用 ECM を多重化するタイミングを制御する別の方法（ECM 多重化制御部 7 の多重化制御信号によらない方法）として、I ピクチャ検出部 5 にて I ピクチャを検出後、この多重化部 15 で暗号化コンテンツをバッファリングしておき、I ピクチャの先頭パケットが含まれている TS パケットの直前に当該蓄積再生用 ECM を多重化してもよい。ただし、この方法では、多重化部 15 において、暗号化コンテンツから I ピクチャを検出できる検出手段を備える必要があり、さらに、暗号化コンテンツをバッファリングする記録手段を備える必要がある。

【0050】

そこで、ECM 多重化制御部 7 では、I ピクチャ検出部 5 にて検出された I ピクチャに基づいて、次の I ピクチャがあると想定される地点の数パケット若しくは数十パケット前に蓄積再生用 ECM を多重化するために、I ピクチャ検出部 5 にて所定のパケット数が通過した後（所定の時間が経過した後）、蓄積再生用 ECM を多重化する構成としてもよい。このように構成することによって、多重化部 15 では、I ピクチャを認識する必要がなくなり、I ピクチャの先頭パケットより数パケット若しくは数十パケット前に蓄積再生用 ECM を多重化することができる。

【0051】

このコンテンツ送信装置 1 によれば、エンコーダ 3 で、映像音声コンテンツがエンコード（符号化）されて、映像音声コンテンツストリーム（TS）とされる。I ピクチャ検出部 5 で、I ピクチャの先頭のパケットが検出される。また、スクランブル部 11 で、映像音声コンテンツストリーム（TS）がスクランブル鍵  $K_s$  で暗号化され、暗号化コンテンツとされる。また、ECM 生成部 13 で、スクランブル鍵  $K_s$  を含む暗号鍵関連情報が受信側と共通の秘密鍵によって暗号化された受信用 ECM および蓄積再生用 ECM が生成され、多重化部 15 に出力される。さらにまた、ECM 多重化制御部 7 で、I ピクチャ検出部 5 にて検出された I ピクチャに基づいて、蓄積再生用 ECM を暗号化コンテンツに多重する際の多重化制御信号が生成される。そして、多重化部 15 で、暗号化コンテンツと、受信用 ECM と、多重化制御信号に基づいた蓄積再生用 ECM とが多重化されて多重化コンテンツとされる。

【0052】

このため、ECM 生成部 13 で受信側と共通の秘密鍵でスクランブル鍵  $K_s$  が暗号化されているので、このスクランブル鍵  $K_s$  が不正に取得されるおそれが無くなり、さらに、I ピクチャの位置に従って蓄積再生用 ECM が暗号化コンテンツに多重化されているので、暗号化コンテンツの早送り再生や早巻き戻し再生等の特殊再生を行ったとしても、蓄積再

生用 ECM を検出して、暗号化コンテンツを復号するためのスクランブル鍵  $K_s$  を即座に取得することができ、特殊再生の性能を高性能に維持し、動作を安定させることができる。

#### 【0053】

(コンテンツ特殊再生装置の構成)

図2にコンテンツ特殊再生装置(コンテンツ再生装置の一実施の形態)のブロック図を示す。この図2に示すように、コンテンツ特殊再生装置17は、受信機本体19と、セキュリティモジュール21とを備えている。

#### 【0054】

このコンテンツ特殊再生装置17は、送信側のコンテンツ送信装置1から送信された多重化コンテンツを一旦蓄積した後、当該多重化コンテンツに多重化されている暗号化コンテンツの早送り再生や早巻き戻し再生等の特殊再生を可能にするものである。

#### 【0055】

受信機本体19は、多重化コンテンツ受信分離部23と、デスクランブル部25と、デコーダ27と、蓄積部29と、分離部31とを備えている。

#### 【0056】

多重化コンテンツ受信分離部23は、送信側から送信された多重化コンテンツ(MPEG2-TS)を受信して、リアルタイム再生を行う場合には、多重化コンテンツに含まれている受信用ECMと、暗号化コンテンツおよび蓄積再生用ECMとを分離し、受信用ECMをセキュリティモジュール21に出力し、暗号化コンテンツをデスクランブル部25に出力すると共に、蓄積部29に蓄積する場合、分離せずに多重化コンテンツのまま蓄積部29に出力するものである。なお、この多重化コンテンツ受信分離部23の特許請求の範囲に記載した多重化コンテンツ受信分離手段に相当するものである。

#### 【0057】

デスクランブル部25は、多重化コンテンツ受信分離部23または蓄積部29から出力された暗号化コンテンツ(MPEG2-TS)を、セキュリティモジュール21から出力されたスクランブル鍵 $K_s$ でデスクランブル(復号)した符号化コンテンツをデコーダ27に出力するものである。なお、このデスクランブル部25の特許請求の範囲に記載した暗号化コンテンツ復号手段に相当するものである。

#### 【0058】

デコーダ27は、デスクランブル部25でデスクランブル(復号)された符号化コンテンツを復元したコンテンツを外部に出力するものである。なお、このデコーダ27の特許請求の範囲に記載したコンテンツ復元手段に相当するものである。

#### 【0059】

蓄積部29は、多重化コンテンツ受信分離部23にて受信し、分離した暗号化コンテンツおよび蓄積再生用ECMを蓄積するためのものである。この蓄積部29は、コンテンツ特殊再生装置17で受信した多重化コンテンツを蓄積すると当該装置17のユーザーが決定した場合に使用されるものである。なお、この蓄積部29の特許請求の範囲に記載した蓄積手段に相当するものである。

#### 【0060】

分離部31は、蓄積部29に蓄積された暗号化コンテンツを再生する際に、当該暗号化コンテンツおよび蓄積再生用ECMを分離して、暗号化コンテンツをデスクランブル部25に、蓄積再生用ECMをセキュリティモジュール21に出力するものである。この分離部31は、コンテンツ特殊再生装置17で受信した多重化コンテンツを蓄積すると当該装置17のユーザーが決定した後、一旦蓄積部29に蓄積した暗号化コンテンツを読み出して再生する(視聴する)際に使用されるものである。なお、この分離部31の特許請求の範囲に記載した分離手段に相当するものである。

#### 【0061】

セキュリティモジュール21は、ICカード等によって構成され、内部に記録した情報が外部より読取不可能に構成されており、耐タンパー性(耐衝撃性)を備えたモジュールで

あり、復号部 33 を備えている。

【0062】

復号部 33 は、受信機本体 19 の多重化コンテンツ受信分離部 23 から出力された受信用 ECM および分離部 31 から出力された蓄積再生用 ECM を、送信側のコンテンツ送信装置 1 と共通に備えられている秘密鍵によって、復号し、スクランブル鍵 K<sub>s</sub> を取得して、受信機本体 19 のデスクランブル部 25 に出力するものである。この復号部 33 が特許請求の範囲に記載した ECM 復号手段に相当するものである。

【0063】

このコンテンツ特殊再生装置 17 によれば、多重化コンテンツ受信分離部 23 で、送信側であるコンテンツ送信装置 1 から送信された多重化コンテンツが受信され、受信用 ECM と、蓄積再生用 ECM および暗号化コンテンツとに分離される。そして、リアルタイム再生の場合、セキュリティモジュール 21 の復号部 33 で、受信用 ECM が復号され、スクランブル鍵 K<sub>s</sub> が取得され、デスクランブル部 25 に出力される。続いて、このデスクランブル部 25 で暗号化コンテンツがスクランブル鍵 K<sub>s</sub> によってデスクランブル（復号）され、デコード 27 で復元されて出力される。また、蓄積後再生する場合、蓄積部 29 に蓄積されている暗号化コンテンツおよび蓄積再生用 ECM が分離部 31 で分離され、セキュリティモジュール 21 の復号部 33 で、蓄積再生用 ECM が復号され、スクランブル鍵 K<sub>s</sub> が取得され、デスクランブル部 25 に出力される。続いて、このデスクランブル部 25 で暗号化コンテンツがスクランブル鍵 K<sub>s</sub> によってデスクランブル（復号）され、デコード 27 で復元されて出力される。

【0064】

このため、セキュリティモジュール 21 の復号部 33 で送信側と共通の秘密鍵でスクランブル鍵 K<sub>s</sub> が復号されるので、このスクランブル鍵 K<sub>s</sub> が不正に取得されるおそれが無くなり、さらに、蓄積部 29 に暗号化コンテンツを蓄積した後に早送り再生や早巻き戻し再生等の特殊再生を行う場合、スクランブル鍵 K<sub>s</sub> が含まれている蓄積再生用 ECM が I ピクチャの位置に従って暗号化コンテンツに多重化されているので、この多重化されている蓄積再生用 ECM を即座に検出して、スクランブル鍵 K<sub>s</sub> を取得することができ、特殊再生の性能を高性能に維持し、当該装置 17 の動作を安定させることができる。

【0065】

（コンテンツ送信装置の動作）

次に、図 3 に示すフローチャートを参照して、コンテンツ送信装置 1 の動作について説明する（適宜、図 1 参照）。

まず、コンテンツ送信装置 1 に入力された映像音声コンテンツがエンコーダ 3 でエンコード（符号化）されて、符号化コンテンツとして I ピクチャ検出部 5 およびスクランブル部 11 に出力される（S1）。そしてまず、I ピクチャ検出部 5 において、符号化コンテンツから基準コンテンツ（I ピクチャ、複数の基準コンテンツ [複数の I ピクチャ]）が検出され、ECM 多重化制御部 7 に出力される（S2）。

【0066】

そして、ECM 多重化制御部 7 で、基準コンテンツに基づいて（I ピクチャの先頭パケットの数パケット若しくは数十パケット前）、多重化制御信号が生成され、多重化部 15 に出力される（S3）。

【0067】

また、鍵生成部 9 では、スクランブル鍵 K<sub>s</sub> が生成され、スクランブル部 11 および ECM 生成部 13 に出力される（S4）。すると、スクランブル部 11 で符号化コンテンツがスクランブル鍵 K<sub>s</sub> によってスクランブルされ、暗号化コンテンツとして多重化部 15 に出力される（S5）。

【0068】

また、ECM 生成部 13 で、スクランブル鍵 K<sub>s</sub> を含む暗号鍵関連情報が秘密鍵によって暗号化された受信用 ECM および蓄積再生用 ECM が生成され、多重化部 15 に出力される（S6）。その後、多重化部 15 で、ECM 多重化制御部 7 で生成された多重化制御信

号に基づいて、受信用ECM、蓄積再生用ECMおよび暗号化コンテンツが多重化され、多重化コンテンツ(MPEG2-TS)として出力(送信)される(S7)。

【0069】

(コンテンツ特殊再生装置の動作[受信・蓄積・通常再生時])

次に、図4に示すフローチャートを参照して、コンテンツ特殊再生装置17の受信・蓄積・通常再生時の動作について説明する(適宜、図2参照)。

まず、コンテンツ特殊再生装置17の多重化コンテンツ受信分離部23で多重化コンテンツが受信される(S11)。続いて、この多重化コンテンツに多重化されている暗号化コンテンツを復号して視聴するかどうか当該装置17のユーザーの判断に委ねられ、当該装置17のユーザーがすぐに(リアルタイムに)暗号化コンテンツを復号して視聴するとして当該装置17を操作した場合(すぐにコンテンツ再生すると当該装置17が判定した場合、S12、Yes)、多重化コンテンツ受信分離部23で、多重化コンテンツが分離され、受信用ECMがセキュリティモジュール21の復号部33に出力され、暗号化コンテンツがデスクランブル部25に出力される(S13)。

【0070】

そして、セキュリティモジュール21の復号部33で受信用ECMが復号され、スクランブル鍵Ksが取得され、デスクランブル部25に出力される(S14)。

【0071】

すると、デスクランブル部25で、暗号化コンテンツがデスクランブルされ、符号化コンテンツがデコーダ27に出力され(S15)、デコーダ27で符号化コンテンツが復元され、コンテンツとして出力される(S16)。

【0072】

また、当該装置17のユーザーが一旦暗号化コンテンツを蓄積部29に蓄積した後に、復号して視聴するとして当該装置17を操作した場合(すぐにコンテンツ再生すると当該装置17が判定しなかった場合、S12、No)、多重化コンテンツ受信分離部23で多重化コンテンツが分離され、蓄積再生用ECMおよび暗号化コンテンツが蓄積部29に出力され、この蓄積部29で蓄積される(S17)。

【0073】

その後、当該装置17のユーザーによって、蓄積部29に蓄積した暗号化コンテンツを再生すると判断した場合(再生するとして当該装置17を操作した場合)、分離部31で、蓄積部29に蓄積されている蓄積再生用ECMと、暗号化コンテンツとが読み出されて分離され、蓄積再生用ECMがセキュリティモジュール21に出力され、暗号化コンテンツがデスクランブル部25に出力される(S19)。

【0074】

そしてまず、セキュリティモジュール21の復号部33で蓄積再生用ECMが復号され、スクランブル鍵Ksが取得され、このスクランブル鍵Ksがデスクランブル部25に出力される(S20)。続いて、デスクランブル部25で暗号化コンテンツがスクランブル鍵Ksによってデスクランブル(復号)され、符号化コンテンツとしてデコーダ27に出力され(S15)、デコーダ27で符号化コンテンツが復元され、コンテンツとして出力される(S16)。

【0075】

(コンテンツ特殊再生装置の動作[特殊再生時])

次に、図5に示すフローチャートを参照して、コンテンツ特殊再生装置17の特殊再生時の動作について説明する(適宜、図2参照)。

まず、暗号化コンテンツに含まれている(暗号化されている映像音声コンテンツストリーム)に含まれているPATが、図示を省略した主制御部によって検索され、検出される(S21)。続いて、このPATで記述されている全PMTのPIDに基づいて、PMTが図示を省略した主制御部によって検索され、検出される(S22)。また、PMTで記述されている情報に基づいて、ECMが図示を省略した主制御部によって検索され、検出される(S23)。

10

20

30

40

50

## 【0076】

そして、デスクランブル部25で、分離部31で分離された暗号化コンテンツ（暗号化されたTS）を復号しながらIフレーム（Iピクチャ）が検索され、検出されて、デコーダ27に出力される（S24）。さらに、次のIフレーム（Iピクチャ）を復号するために必要なECMまでスキップされる（おおよその時間から主制御部（図示せず）で算出したバイト数スキップ）（S25）。

## 【0077】

特殊再生を終了するか否か判定され（S26）、終了すると判定されない場合（S26、No）、S23に戻り、終了すると判定された場合（S26、Yes）、特殊再生が終了される。

10

## 【0078】

（コンテンツの特殊再生とECMとについて）

最後に、図6～図8を参照して、コンテンツの特殊再生とECMとについて説明する（適宜、図2参照）。

図6は、コンテンツ特殊再生装置17の蓄積部29に蓄積されている暗号化コンテンツおよび蓄積再生用ECM（一本のTS）を示したものである。この図6に示すように、まず、時間軸にそって、ECM（ECM2；蓄積再生用ECM）が検索され、検索されると、この検索されたECM（ECM2；蓄積再生用ECM）からスクランブル鍵Ksが復号部33で取得される。続いて、このスクランブル鍵Ksで暗号化コンテンツが復号され、符号化コンテンツとされて、この符号化コンテンツに含まれているIピクチャが検索され検

20

## 【0079】

そして、再生間隔では、再生（通常再生）、スキップ等の「早送り再生」がおこなわれ、この間では、GOP（Group of pictures；Iピクチャを少なくとも1個含む画面群）が再生されることになり、さらに、次のGOPが再生される前に、次のECM（ECM2；蓄積再生用ECM）が検索され、以下同様にこのECM（ECM2；蓄積再生用ECM）からスクランブル鍵Ksが取得される。

## 【0080】

また、図7にECMをIピクチャ同期で多重化した方式を示す。この図7に示したように、Iピクチャ先頭パケットの直前に、当該Iピクチャに同期したECM2（蓄積再生用ECM）が挿入されている。

30

## 【0081】

さらにまた、図8にECM1およびECM2を混合した方式を示す。この図8に示すように、ECM1（受信用ECM）とIピクチャの先頭パケットとの間にECM2（蓄積再生用ECM）が挿入されており、ECM1同士の間隔は一定間隔（例えば、100ms）である。

## 【0082】

（コンテンツ送信装置およびコンテンツ特殊再生装置の効果について）

以上、各図面（図1～図8）に基づいて説明した本発明の一実施の形態であるコンテンツ送信装置1およびコンテンツ特殊再生装置17の効果について、まとめておく。

40

## 【0083】

コンテンツ送信装置1で、Iピクチャの先頭パケットを含んでいるTSパケットに同期するように蓄積再生用ECMを、多重化部15で多重化することにより、スクランブル部11でスクランブルしたTSパケットがIピクチャであることを示す情報を当該TSパケットの非暗号化部に入れることなしに、Iピクチャの先頭パケットが含まれているTSパケットのおおよその位置が判明する。

## 【0084】

このため、スクランブル部11でスクランブルしたTSパケットの安全性（秘匿性）を損なうことなしに、受信側（再生側）のコンテンツ特殊再生装置17において、Iピクチャの検索時間を短縮することができ、早送り再生や早巻き戻し再生等の特殊再生をするとき

50

に安定した動作を実現することができる（ユーザーにとって、十分満足のいくレベルを実現できる）。

【0085】

また、送信側のコンテンツ送信装置1の多重化部15において、一定間隔で符号化コンテンツに多重化する受信用ECMと、Iピクチャに同期して多重化する（多重化制御信号に基づいて）蓄積再生用ECMとを多重化することにより、受信側のコンテンツ特殊再生装置17において、受信時または選局時の応答速度の低下させることを防止することができる。

【0086】

さらに、蓄積再生用ECMは、Iピクチャに同期しており、送信側のコンテンツ送信装置1からは最小限必要なスクランブル鍵Ksを含む暗号鍵関連情報を送信しているので、放送帯域を効率的に使用することができ、且つ、蓄積部29に蓄積した後再生する場合に、GOPを最小単位として、コンテンツの一部分のみを通常再生および特殊再生（早送り再生、早巻き戻し再生）することができる。

【0087】

さらにまた、この実施の形態では、送信側のコンテンツ送信装置1において、ECMに含まれている暗号鍵関連情報（スクランブル鍵Ks関連情報）に変更を加えずに、受信側のコンテンツ特殊再生装置17において、Iピクチャの検索時間を軽減させているので、1秒間に表示されるIピクチャ数を所定の値にした際に、Iピクチャのスキップ数に制限なく、複数枚のIピクチャをスキップさせた非常に高速な早送り再生や早巻き戻し再生を実現することができる。

【0088】

以上、一実施形態に基づいて本発明を説明したが、本発明はこれに限定されるものではない。

例えば、コンテンツ送信装置1およびコンテンツ特殊再生装置17の各構成の処理を一つずつの過程と捉えたコンテンツ送信方法およびコンテンツ再生方法とみなすことや、各構成の処理を汎用的なコンピュータ言語で記述したコンテンツ送信プログラムおよびコンテンツ再生プログラムとみなすことは可能である。これらの場合、コンテンツ送信装置1およびコンテンツ特殊再生装置17と同様の効果を得ることができる。

【0089】

【発明の効果】

請求項1、2、3記載の発明によれば、受信用ECMおよび蓄積再生用ECMに暗号鍵が暗号化されているので、この暗号鍵が不正に取得されるおそれが無くなり、さらに、基準コンテンツの位置に従って蓄積再生用ECMが暗号化コンテンツに多重化されているので、暗号化コンテンツの早送り再生や早巻き戻し再生等の特殊再生を行ったとしても、蓄積再生用ECMを即座に検出して、暗号化コンテンツを復号するための暗号鍵を取得することができ、特殊再生の性能を高性能に維持し、動作を安定させることができる。

【0090】

請求項4、5、6記載の発明によれば、暗号鍵が含まれている蓄積再生用ECMが基準コンテンツの位置に従って暗号化コンテンツに多重化されているので、暗号化コンテンツおよび蓄積再生用ECMを蓄積した後早送り再生や早巻き戻し再生等の特殊再生を行う場合、この多重化されている蓄積再生用ECMを即座に検出して、暗号鍵を取得することができ、特殊再生の性能を高性能に維持し、当該装置の動作を安定させることができる。

【図面の簡単な説明】

【図1】本発明による一実施の形態であるコンテンツ送信装置のブロック図である。

【図2】本発明の一実施の形態であるコンテンツ特殊再生装置のブロック図である。

【図3】図1に示したコンテンツ送信装置の動作を説明したフローチャートである。

【図4】図2に示したコンテンツ特殊再生装置の動作（受信、蓄積、通常再生動作）を説明したフローチャートである。

【図5】図2に示したコンテンツ特殊再生装置の動作（特殊再生動作）を説明したフロー

10

20

30

40

50



チャートである。

【図6】暗号化コンテンツおよび蓄積再生用ECM（一本のTS）を示した図である。

【図7】蓄積再生用ECMをIピクチャ同期で多重化した方式を示した図である。

【図8】受信用ECMおよび蓄積再生用ECMを混合した方式を示した図である。

【図9】暗号化コンテンツに一定間隔で多重化される従来のECMについて示した図である。

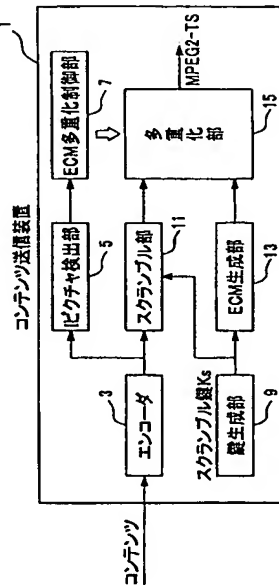
【符号の説明】

- |    |               |
|----|---------------|
| 1  | コンテンツ送信装置     |
| 3  | エンコーダ         |
| 5  | Iピクチャ検出部      |
| 7  | ECM多重化制御部     |
| 9  | 鍵生成部          |
| 11 | スクランブル部       |
| 13 | ECM生成部        |
| 15 | 多重化部          |
| 17 | コンテンツ特殊再生装置   |
| 19 | 受信機本体         |
| 21 | セキュリティモジュール   |
| 23 | 多重化コンテンツ受信分離部 |
| 25 | デスクランブル部      |
| 27 | デコーダ          |
| 29 | 蓄積部           |
| 31 | 分離部           |
| 33 | 復号部           |

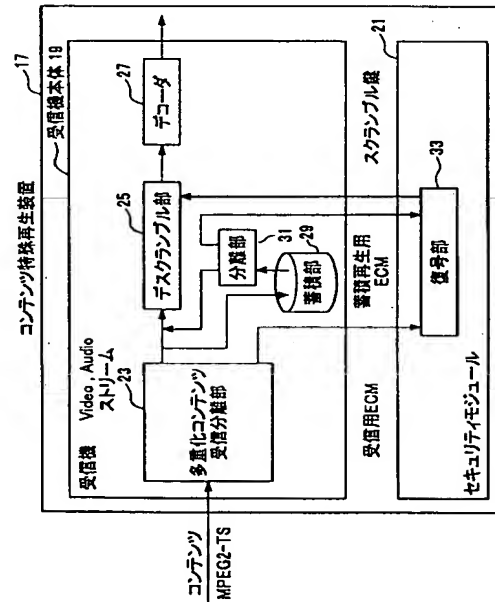
10

20

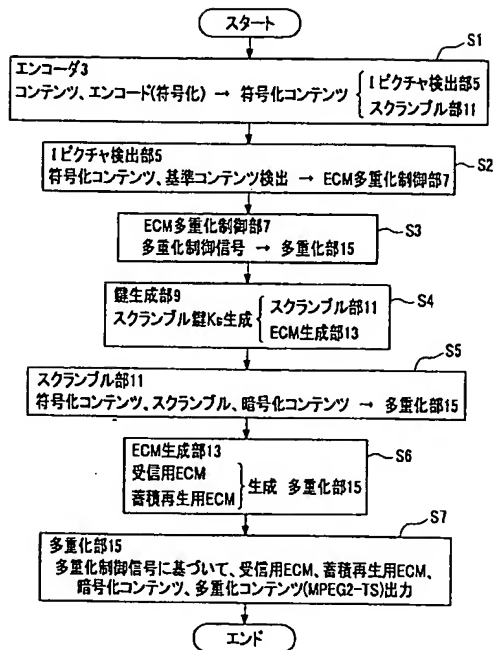
【図1】



【図2】

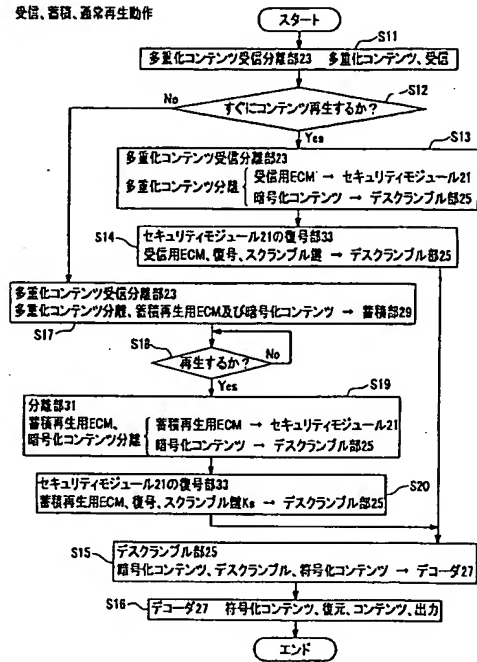


【図 3】

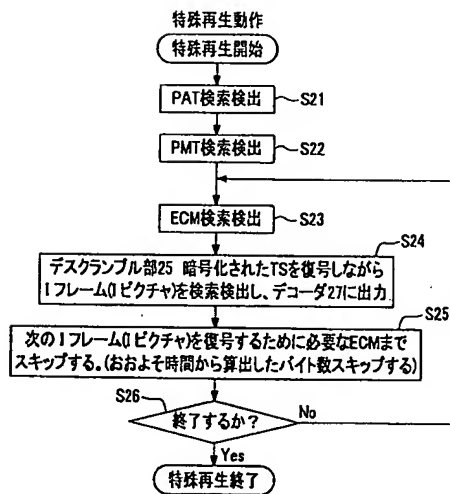


【図 4】

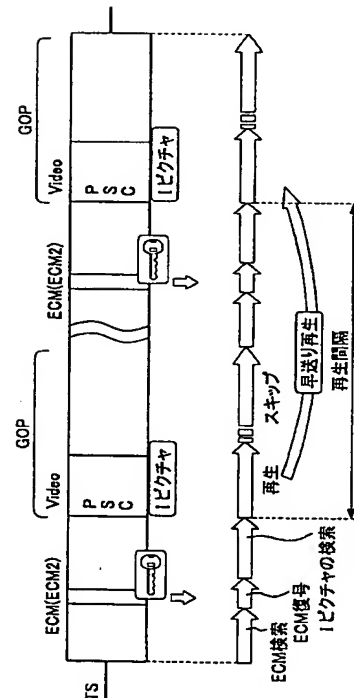
受信、蓄積、通常再生動作



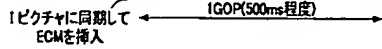
【図 5】



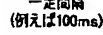
【図 6】



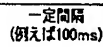
### ECMを1ピクチャ同期で多重した方式



### 両者を混合した方式



### 現在の限定受信方式



## フロントページの続き

(72)発明者 馬場 秋継

東京都世田谷区砧一丁目10番11号

日本放送協会 放送技術研究所内

(72)発明者 藤井 亜里砂

東京都世田谷区砧一丁目10番11号

日本放送協会 放送技術研究所内

Fターム(参考) 5C053 FA20 FA30 GB06 GB08 GB38 HA24 HA25 JA30 LA07 LA14

5C063 AB03 AC01 AC05 AC10 DA20 DB10

5C064 CA18 CC01 CC06

5J104 AA12 PA05 PA14